PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/30, G06F 7/72 — A1

(11) Numéro de publication internationale: **WO 00/59156**

(43) Date de publication internationale: 5 octobre 2000 (05.10.00)

(21) Numéro de la demande internationale: PCT/FR00/00603

(22) Date de dépôt international: 13 mars 2000 (13.03.00)

(30) Données relatives à la priorité:
99/03921 26 mars 1999 (26.03.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS [FR/FR]; Nonnenmacher, Bernard, Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F–13881 Gémenos (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(US seulement)*: CORON, Jean–Sébastien [FR/FR]; 4 rue Léon de Lagrange, F–75015 Paris (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus, Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F–13881 Gémenos (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Avec rapport de recherche internationale.

(54) Title: COUNTERMEASURE PROCEDURES IN AN ELECTRONIC COMPONENT IMPLEMENTING AN ELLIPTICAL CURVE TYPE PUBLIC KEY ENCRYPTION ALGORITHM

(54) Titre: PROCEDES DE CONTRE–MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE

(57) **Abstract**

Elliptical curve based cryptographic algorithms are public key algorithms offering a shorter calculation time and smaller key sizes in comparison with RSA. The application thereof in a chipcard type environment has proved to be vulnerable to differential power analysis (DPA) attacks. The invention describes a countermeasure procedure enabling positive action to be taken against DPA type attacks. The countermeasure does not reduce performance and is easy to use in a chipcard type component.

(57) **Abrégé**

Les algorithmes cryptographiques à base de courbes elliptiques sont des algorithmes à clef publique présentant sur RSA l'avantage de temps de calcul présentant sur RSA l'avantage de temps de calcul plus faible et de taille de clefs plus petites. Il est apparu que leur application dans le cadre d'un environnement de type carte à puce était vulnérable à des attaques de type DPA (Differential Power Analysis). La présente invention consiste en la description d'un procédé de contre–mesure permettant de se prémunir contre ce type d'attaque DPA. Cette contre–mesure ne diminue pas les performances et est facilement utilisable dans un composant de type carte à puce.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDES DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme de chiffrement à clé publique de type courbe elliptique.

Dans le modèle classique de la cryptographie à clef secrète, deux personnes désirant communiquer par l'intermédiaire d'un canal non sécurisé doivent au préalable se mettre d'accord sur une clé secrète de chiffrement K. La fonction de chiffrement et la fonction de déchiffrement utilisent la même clef K. L'inconvénient du système de chiffrement à clé secrète est que ledit système requiert la communication préalable de la clé K entre les deux personnes par l'intermédiaire d'un canal sécurisé, avant qu'un quelconque message chiffré ne soit envoyé à travers le canal non sécurisé. Dans la pratique, il est généralement difficile de trouver un canal de communication parfaitement sécurisé, surtout si la distance séparant les deux personnes est importante. On entend par canal sécurisé un canal pour lequel il est impossible de connaître ou de modifier les informations qui transitent par ledit canal. Un tel canal sécurisé peut être réalisé par un câble reliant deux terminaux, possédés par les deux dites personnes.

Le concept de cryptographie à clef publique fut inventé par Whitfield DIFFIE et Martin HELLMAN en 1976. La cryptographie à clef publique permet de résoudre le problème de la distribution des clefs à travers un canal non sécurisé. Le principe de la cryptographie à clef publique consiste à utiliser une paire de clefs, une clef publique de chiffrement et une clef privée de déchiffrement. Il doit être calculatoirement infaisable de trouver la clef privée de déchiffrement à partir de la clef publique de chiffrement. Une personne A désirant communiquer une information à une personne B utilise la clef publique de chiffrement de la personne B. Seule la personne B possède la clef privée associée à sa clef publique. Seule la personne B est donc capable de déchiffrer le message qui lui est adressé.

Un autre avantage de la cryptographie à clé publique sur la cryptographie à clé secrète est que la cryptographie à clef publique permet l'authentification par l'utilisation de signature électronique.

La première réalisation de schéma de chiffrement à clef publique fut mis au point en 1977 par Rivest, Shamir et Adleman, qui ont inventé le système de chiffrement RSA. La sécurité de RSA repose sur la difficulté de factoriser un grand nombre qui est le produit de deux nombres premiers.

Depuis, de nombreux systèmes de chiffrement à clef publique ont été proposés, dont la sécurité repose sur différents problèmes calculatoires : (cette liste n'est pas exhaustive).

- Sac à dos de Merckle-Hellman :

Ce système de chiffrement est basé sur la difficulté du problème de la somme de sous-ensembles.

- McEliece :

Ce système de chiffrement est basé sur la théorie des codes algébriques. Il est basé sur le problème du décodage de codes linéaires.

- ElGamal :

Ce système de chiffrement est basé sur la difficulté du logarithme discret dans un corps fini.

- Courbes elliptiques :

Le système de chiffrement à courbe elliptique constitue une modification de systèmes cryptographiques existant pour les appliquer au domaine des courbes elliptiques.

L'utilisation de courbes elliptiques dans des systèmes cryptographiques fut proposé indépendamment par Victor Miller et Neal Koblitz en 1985. Les applications réelles des courbes elliptiques ont été envisagées au début des années 1990.

L'avantage de cryptosystèmes à base de courbe elliptique est qu'ils fournissent une sécurité équivalente aux autres cryptosystèmes mais avec des tailles de clef moindres. Ce gain en taille de clé implique une diminution des besoins en mémoire et une réduction des temps de calcul, ce qui rend l'utilisation des courbes elliptiques particulièrement adaptées pour des applications de type carte à puce.

Une courbe elliptique sur un corps fini GF(q^n) (q étant un nombre premier et n un entier) est l'ensemble des points (x,y) avec x l'abscisse et y l'ordonnée appartenant à GF(q^n) solution de l'équation :

$y^2=x^3+a*x+b$

si q est supérieur ou égal à 3

et $y^2+x*y=x^3+a*x^2+b$

si q=2.

Il existe 2 procédés pour représenter un point d'une courbe elliptique :

Premièrement, la représentation en coordonnées affine; dans ce procédé, un point P de la courbe elliptique est représenté par ses coordonnées (x,y).

Deuxièment, la représentation en coordonnées projectives.

L'avantage de la représentation en coordonnées projectives est qu'elle permet d'éviter les divisions dans le corps fini, lesdites divisions étant les opérations les plus coûteuses en temps de calcul.

La représentation en coordonnés projectives le plus couramment utilisée est celle consistant à représenter un point P de la courbe elliptique par les coordonnées (X,Y,Z), telles que x=X/Z et y=Y/Z^3.
Les coordonnées projectives d'un point ne sont pas uniques parce que le triplet (X,Y,Z) et le triplet (λ^2*X, λ^3*Y, λ*Z) représentent le même point quelque soit l'élément λ appartenant au corps fini sur lequel est défini la courbe elliptique.

Les 2 classes de courbes les plus utilisées en cryptographie sont les suivantes :

1) Courbes définies sur le corps fini GF(p) (ensemble des entiers modulo p, p étant un nombre premier) ayant pour équation y^2=x^3+a*x+b

2) Courbes définies sur le corps fini GF(2^n) ayant pour équation
y^2+x*y=x^3+a*x^2+b

Pour chacune de ces deux classes de courbes, on définit les opérations d'addition de point et de doublement de point.
L'addition de point est l'opération qui étant donné deux points P et Q calcule la somme R=P+Q, R étant un point de la courbe dont les coordonnées s'expriment à l'aide des coordonnées des points P et Q suivant des formules dont l'expression est donnée dans l'ouvrage

" Elliptic curve public key cryptosystem " par Alfred J. Menezes.
Le doublement de point est l'opération qui, étant donné un point P, calcule le point R=2*P, R étant un point de la courbe dont les coordonnées s'expriment à l'aide des coordonnées du point P suivant des formules dont l'expression est donnée dans l'ouvrage " Elliptic curve public key cryptosystem " par Alfred J. Menezes.

Les opérations d'addition de point et de doublement de point permettent de définir une opération de multiplication scalaire : étant donné un point P appartenant à une courbe elliptique et un entier d, le résultat de la multiplication scalaire de P par d est le point Q tel que Q=d*P=P+P+...+P d fois.

La sécurité des algorithmes de cryptographie sur courbes elliptiques est basée sur la difficulté du problème du logarithme discret sur courbes elliptiques, ledit problème consistant à partir de deux points Q et P appartenant à une courbe elliptique E, de trouver, s'il existe, un entier x tel que Q=x*P

Il existe de nombreux algorithmes cryptographiques basés sur le problème du logarithme discret. Ces algorithmes sont facilement transposables aux courbes elliptiques.

Ainsi, il est possible de mettre en œuvre des algorithmes assurant l'authentification, la confidentialité, le contrôle d'intégrité et l'échange de clé.

Un point commun à la plupart des algorithmes cryptographiques basés sur les courbes elliptiques est qu'ils comprennent comme paramètre une courbe elliptique définie sur un corps fini et un point P appartenant à cette courbe elliptique. La clé privée est un entier d choisi aléatoirement. La clef publique est un point de la courbe Q tel que Q=d*P. Ces algorithmes cryptographiques font généralement intervenir une multiplication scalaire dans le calcul d'un point R=d*T où d est la clef secrète.

Dans le paragraphe ci dessous, on décrit un algorithme de chiffrement à base de courbe elliptique. Ce schéma est analogue au schéma de chiffrement d'El Gamal. Un message m est chiffré de la manière suivante :

Le chiffreur choisit un entier k aléatoirement et calcule les points k*P=(x1,y1) et k*Q=(x2,y2) de la courbe, et l'entier c= x2 + m. Le chiffré de m est le triplet (x1,y1,c).
Le déchiffreur qui possède d déchiffre m en calculant :
(x'2,y'2)=d(x1,y1) et m=c-x'2

Pour réaliser les multiplications scalaires nécessaires dans les procédés de calcul décrits précédemment, plusieurs algorithmes existent :

- Algorithme " double and add " ;
- Algorithme " addition-soustraction "
- Algorithme avec chaines d'addition ;
- Algorithme avec fenêtre ;
- Algorithme avec représentation signée.

Cette liste n'est pas exhaustive. L'algorithme le plus simple et le plus utilisé est l'algorithme " double and add ". L'algorithme " double and add " prend en entrée un point P appartenant à une courbe elliptique donnée et un entier d. L'entier d est noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme retourne en sortie le point Q=d.P.

L'algorithme " double and add " comporte les 3 étapes suivantes :

1) Initialiser le point Q avec la valeur P
2) Pour i allant de t-1 à 0 exécuter :
2a) Remplacer Q par 2Q
2b) Si d(i)=1 remplacer Q par Q+P
3) Retourner Q.

Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé publique du type courbe elliptique était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé privée de déchiffrement. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation de courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à l'instruction montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur 0 ou 1. L'attaque de type DPA permet donc d'obtenir des informations supplémentaires sur les données intermédiaires manipulées par le microprocesseur de la carte lors de l'exécution d'un algorithme cryptographique. Ces informations supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme de déchiffrement, rendant le système cryptographique non sûr.

Dans la suite de ce document on décrit un procédé d'attaque DPA sur un algorithme de type courbe elliptique réalisant une opération du type multiplication scalaire d'un point P par un entier d, l'entier d étant la clé secrète. Cette attaque permet de révéler directement la clé secrète d. Elle compromet donc gravement la sécurité de l'implémentation de courbes elliptiques sur une carte à puce.

La première étape de l'attaque est l'enregistrement de la consommation de courant correspondant à l'exécution de l'algorithme " double and add " décrit précédemment pour N points distincts P(1),..., P(N). Dans un algorithme à base de courbes elliptiques, le microprocesseur de la carte à puce va effectuer N multiplications scalaires d.P(1),...,d.P(N).

Pour la clarté de la description de l'attaque, on commence par décrire une méthode permettant d'obtenir la valeur du bit d(t-1) de la clé secrète d, où (d(t),d(t-1),..., d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. On donne ensuite la description d'un algorithme qui permet de retrouver la valeur de d.

On groupe les points P(1) à P(N) suivant la valeur du dernier bit de l'abscisse de 4.P, où P désigne un des points P(1) à P(N). Le premier groupe est constitué des points P tels que le dernier bit de l'abscisse de 4.P est égal à 1.

Le second groupe est constitué des points P tels que le dernier bit de l'abscisse de 4.P est égal à 0. On calcule la moyenne des consommations de courant correspondant à chacun des deux groupes, et on calcule la courbe de différence entre ces deux moyennes.

Si le bit d(t-1) de d est égal à 0, alors l'algorithme de multiplication scalaire précédemment décrit calcule et met en mémoire la valeur de 4.P. Cela signifie que lors de l'exécution de l'algorithme dans une carte à puce, le microprocesseur de la carte va effectivement calculer 4.P. Dans ce cas, dans le premier groupe de message le dernier bit de la donnée manipulée par le microprocesseur est toujours à 1, et dans le deuxième groupe de message le dernier bit de la donnée manipulée est toujours à 0. La moyenne des consommations de courant correspondant à chaque groupe est donc différente. Il apparaît donc dans la courbe de différence entre les 2 moyennes un pic de différentiel de consommation de courant.

Si au contraire le bit d(t-1) de d est égal à 1, l'algorithme d'exponentiation décrit précédemment ne calcule pas le point 4.P. Lors de l'exécution de l'algorithme par la carte à puce, le microprocesseur ne manipule donc jamais la donnée 4.P. Il n'apparaît donc pas de pic de différentiel de consommation.

Cette méthode permet donc de déterminer la valeur du bit d(t-1) de d.

L'algorithme décrit dans le paragraphe suivant est une généralisation de l'algorithme précédant. Il permet de déterminer la valeur de la clé secrète d.

On définit l'entrée par N points notés P(1) à P(N) correspondant à N calculs réalisés par la carte à puce et la sortie par un entier h.

Ledit algorithme s'effectue de la manière suivante en trois étapes.

1) Exécuter h=1 ;
2) Pour i allant de t-1 à 1, exécuter :
2)1) Classer les points P(1) à P(N) suivant la valeur du dernier bit de l'abscisse de (4*h).P ;
2)2) Calculer la moyenne de consommation de courant pour chacun des deux groupes ;
2)3) Calculer la différence entre les 2 moyennes ;
2)4) Si la différence fait apparaître un pic de différentiel de consommation, faire h=h*2 ; sinon faire h=h*2+1 ;
3) Retourner h.

L'algorithme précédent fournit un entier h tel que d=2*h ou d=2*h+1. Pour obtenir la valeur de d, il suffit ensuite de tester les deux hypothèses possibles.

L'attaque de type DPA décrite permet donc de retrouver la clé privée d.

Le procédé de l'invention consiste en l'élaboration d'une contre mesure permettant de se prémunir contre l'attaque DPA décrite précédemment. Cette contre mesure utilise la représentation des points de la courbe elliptique en coordonnées projectives.

Comme il a été expliqué précédemment, le représentant d'un point en coordonnées projectives n'est pas unique. Si le corps fini sur lequel est défini la courbe elliptique comprend n élements, il est possible de choisir un représentant parmi n-1 possibles.
En choisissant un représentant aléatoire d'un point sur lequel on effectue un calcul, les valeurs intermédiaires du calcul deviennent elles-mêmes aléatoires et donc imprévisibles de l'extérieur, ce qui rend l'attaque DPA précédemment décrite impossible.

Le procédé de la contre mesure consiste en une modification des opérations d'addition de point et de doublement de point de courbe elliptiques définies sur les corps finis GF(p) pour p premier et GF(2^n). La modification des opérations d'addition de point et de doublement de point de courbes elliptiques définies sur les corps finis GF(p) pour p premier et GF(2^n) s'applique quelque soit l'algorithme utilisé pour réaliser ces opérations.

Le procédé de la contre mesure consiste également en la définition de 4 variantes dans l'opération de multiplication scalaire. Ces 4 variantes s'appliquent quelque soit l'algorithme utilisé pour réaliser l'opération de multiplication scalaire.

Dans ce paragraphe, on décrit la modification de l'algorithme de doublement de point d'une courbe elliptique définie sur le corps fini GF(p), où p est un nombre premier. La courbe elliptique est donc définie par l'équation suivante :

$$y^2=x^3+a*x+b$$

où a et b sont des paramètres entiers fixés au départ.

Les coordonnées projectives du point Q=(X2,Y2,Z2) tel que Q=2.P avec P=(X1,Y1,Z1) sont calculées par le procédé suivant en 6 étapes. Dans chacune des étapes, les calculs sont effectués modulo p.

1) Calculer $M=3*X1^2+a*Z1^4$;
2) Calculer $Z2=2*Y1*Z1$;
3) Calculer $S=4*X1*Y1^2$;
4) Calculer $X2=M^2-2*S$;
5) Calculer $T=8*Y1^4$;
6) Calculer $Y2=M*(S-X2)-T$.

Le procédé de la contre mesure consiste en une modification du procédé précédent.

Le nouveau procédé de doublement de point d'une courbe elliptique définie sur le corps fini GF(p) consiste en les 8 étapes suivantes :

1) Tirer au hasard un entier λ tel que $0<\lambda<p$;
2) Calculer $X'1=\lambda^2*X1$, $Y'1=\lambda^3*Y1$ et $Z'1=\lambda*Z1$;
3) Calculer $M=3*X'1^2+a*Z'1^4$;
4) Calculer $Z2=2*Y'1*Z'1$;
5) Calculer $S=4*X'1*Y'1^2$;
6) Calculer $X2=M^2-2*S$;
7) Calculer $T=8*Y'1^4$;
8) Calculer $Y2=M*(S-X2)-T$.

Plus généralement, le procédé de la contre mesure s'applique quelque soit le procédé (noté par la suite A) utilisé pour réaliser l'opération de doublement de point. Le procédé A est remplacé par le procédé A' en 3 étapes :

Entrée : un point P=(X1,Y1,Z1) représenté en coordonnées projectives.
Sortie : une point Q=(X2,Y2,Z2) représenté en coordonnés projectives tel que Q=2.P

1) Tirer au hasard un entier λ tel que $0<\lambda<p$;
2) Calculer $X'1=\lambda^2*X1$, $Y'1=\lambda^3*Y1$ et $Z'1=\lambda*Z1$, X'1, Y'1 et Z'1 définissant les coordonnées du point P'=(X'1,Y'1,Z'1);
3) Calculer Q=2*P' à l'aide de l'algorithme A.

Les variables manipulées au cours de l'exécution du procédé A' étant aléatoire, l'attaque DPA précédemment décrite ne s'applique plus.

Dans ce paragraphe, on décrit la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini GF(p), où p est un nombre premier.

Les coordonnées projectives du point R=(X2,Y2,Z2) tel que R=P+Q avec P=(X0,Y0,Z0) et Q=(X1,Y1,Z1) sont calculées par le procédé suivant en 12 étapes. Dans chacune des étapes, les calculs sont effectués modulo p.

1) Calculer U0=X0*Z1^2;
2) Calculer S0=Y0*Z1^3;
3) Calculer U1=X1*Z0^2;
4) Calculer S1=Y1*Z0^3;
5) Calculer W=U0-U1;
6) Calculer R=S0-S1;
7) Calculer T=U0+U1;
8) Calculer M=S0+S1;
9) Calculer Z2=Z0*Z1*W;
10) Calculer X2=R^2-T*W^2;
11) Calculer V=T*W^2-2*X2;
12) Calculer 2*Y2=V*R-M*W^3.

Le procédé de la contre mesure consiste en une modification du procédé précédent. Le nouveau procédé d'addition de point d'une courbe elliptique définie sur le corps fini GF(p) consiste en les 16 étapes suivantes :

1) Tirer au hasard un entier λ tel que $0<\lambda<p$;

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par $\lambda*Z0$;

3) Tirer au hasard un entier μ tel que $0<\mu<p$;

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par $\mu*Z1$;

5) Calculer $U0=X0*Z1^2$;

6) Calculer $S0=Y0*Z1^3$;

7) Calculer $U1=X1*Z0^2$;

8) Calculer $S1=Y1*Z0^3$;

9) Calculer $W=U0-U1$;

10) Calculer $R=S0-S1$;

11) Calculer $T=U0+U1$;

12) Calculer $M=S0+S1$;

13) Calculer $Z2=Z0*Z1*W$;

14) Calculer $X2=R^2-T*W^2$;

15) Calculer $V=T*W^2-2*X2$;

16) Calculer $2*Y2=V*R-M*W^3$.

Plus généralement, le procédé de la contre mesure s'applique quelque soit le procédé (noté par la suite A) utilisé pour réaliser l'opération d'addition de point. Le procédé A est remplacé par le procédé A' en 5 étapes :

Entrée : deux points P=(X0,Y0,Z0) et Q=(X1,Y1,Z1) représentés en coordonnées projectives.

Sortie : le point R=(X2,Y2,Z2) représenté en coordonnés projectives tel que R=P+Q

1) Tirer au hasard un entier λ tel que $0<\lambda<p$;

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par $\lambda*Z0$;

3) Tirer au hasard un entier μ tel que $0<\mu<p$;

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par $\mu*Z1$;

5) Calcul de R=P+Q à l'aide de l'algorithme A.

Les variables manipulées au cours de l'exécution du procédé A' étant aléatoire, l'attaque DPA précédemment décrite ne s'applique plus.
Dans ce paragraphe, on décrit la modification de l'algorithme de doublement de point d'une courbe elliptique définie sur le corps fini GF(2^n). La courbe elliptique est donc définie par l'équation suivante :

$$y^2+x*y=x^3+a*x^2+b$$

où a et b sont des paramètres appartenant au corps fini GF(2^n) fixés au départ. On définit c par l'équation:

$$c=b^{(2^{(n-2)})}.$$

Les coordonnées projectives du point Q=(X2,Y2,Z2) tel que Q=2.P avec P=(X1,Y1,Z1) sont calculées par le procédé suivant en 4 étapes. Dans chacune des étapes, les calculs sont effectués dans le corps fini GF(2^n).

1) Calculer Z2=X1*Z1^2;
2) Calculer X2=(X1+c*Z1^2)^4;
3) Calculer U=Z2+X1^2+Y1*Z1;
4) Calculer Y2=X1^4*Z2+U*X2.

Le procédé de la contre mesure consiste en une modification du procédé précédent. Le nouveau procédé de doublement de point d'une courbe elliptique définie sur le corps fini GF(2^n) consiste en les 6 étapes suivantes :

1) Tirer au hasard un élément non nul λ de GF(2^n);
2) Calculer X'1=λ^2*X1, Y'1=λ^3*Y1, Z'1=λ*Z1;
3) Calculer Z2=X'1*Z'1^2;
4) Calculer X2=(X'1+c*Z'1^2)^4;
5) Calculer U=Z2+X'1^2+Y'1*Z'1;
6) Calculer Y2=X'1^4*Z2+U*X2.

Plus généralement, le procédé de la contre mesure s'applique quelque soit le procédé (noté par la suite A) utilisé pour réaliser l'opération de doublement de point. Le procédé A est remplacé par le procédé A' en 3 étapes :

Entrée : un point P=(X1,Y1,Z1) représenté en coordonnées projectives.
Sortie : une point Q=(X2,Y2,Z2) représenté en coordonnés projectives tel que Q=2.P

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Calculer X'1=λ^2*X1, Y'1=λ^3*Y1, Z'1=λ*Z1, X'1, Y'1 et Z'1 définissent les coordonnées du point P'=(X'1,Y'1,Z'1);

3) Calcul de Q=2.P' à l'aide de l'algorithme A.

Les variables manipulées au cours de l'exécution du procédé A' étant aléatoire, l'attaque DPA précédemment décrite ne s'applique plus.

Dans ce paragraphe, on décrit la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini GF(2^n).

Les coordonnées projectives du point R=(X2,Y2,Z2) tel que R=P+Q avec P=(X0,Y0,Z0) et Q=(X1,Y1,Z1) sont calculées par le procédé suivant en 12 étapes. Dans chacune des étapes, les calculs sont effectués dans le corps fini GF(2^n).

1) Calculer U0=X0*Z1^2;
2) Calculer S0=Y0*Z1^3;
3) Calculer U1=X1*Z0^2;
4) Calculer S1=Y1*Z0^3;
5) Calculer W=U0+U1;
6) Calculer R=S0+S1;
7) Calculer L=Z0*W;
8) Calculer V=R*X1+L*Y1;
9) Calculer Z2=L*Z1;
10) Calculer T=R+Z2;
11) Calculer X2=a*Z2^2+T*R+W^3;
12) Calculer Y2=T*X2+V*L^2.

Le procédé de la contre mesure consiste en une modification du procédé précédent. Le nouveau procédé d'addition de point d'une courbe elliptique définie sur le corps fini GF(2^n) consiste en les 14 étapes suivantes :

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par λ*Z0;

3) Tirer au hasard un élément μ non nul de GF(2^n);

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par μ*Z1;

5) Calculer U0=X0*Z1^2;

6) Calculer S0=Y0*Z1^3;

7) Calculer U1=X1*Z0^2;

8) Calculer S1=Y1*Z0^3;

9) Calculer W=U0+U1;

10) Calculer R=S0+S1;

11) Calculer L=Z0*W;

12) Calculer V=R*X1+L*Y1;

13) Calculer Z2=L*Z1;

14) Calculer T=R+Z2;

15) Calculer X2=a*Z2^2+T*R+W^3;

16) Calculer Y2=T*X2+V*L^2;

Plus généralement, le procédé de la contre mesure s'applique quelque soit le procédé (noté par la suite A) utilisé pour réaliser l'opération d'addition de point. Le procédé A est remplacé par le procédé A' en 5 étapes :

Entrée : deux points P=(X0,Y0,Z0) et Q=(X1,Y1,Z1) représentés en coordonnées projectives.

Sortie : le point R=(X2,Y2,Z2) représenté en coordonnés projectives tel que R=P+Q

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par λ*Z0;

3) Tirer au hasard un élément μ non nul de GF(2^n);

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par μ*Z1;

5) Calcul de R=P+Q à l'aide de l'algorithme A.

Les variables manipulées au cours de l'exécution du procédé A' étant aléatoire, l'attaque DPA précédemment décrite ne s'applique plus.

Le procédé de la contre mesure consiste également en la définition de 4 variantes dans l'opération de multiplication scalaire. L'opération de multiplication scalaire fait appel à l'opération de doublement de point noté Do et à l'opération d'addition de point noté Ad. L'opération de doublement de point modifié décrite précédemment est notée Do' et l'opération d'addition de point modifiée décrite précédemment est notée Ad'.

Dans ce paragraphe on décrit la première variante de modification de l'opération de multiplication scalaire. La première variante consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul. Dans le cas de l'utilisation de l'algorithme " double and add ", le procédé modifié de multiplication scalaire est le suivant en 5 étapes. Le procédé prend en entrée un point P et un entier d. L'entier d est noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme retourne en sortie le point Q=d.P.

Cette première variante s'exécute en cinq étapes:

1) Initialiser le point Q avec la valeur P;
2) Remplacer Q par 2.Q en utilisant le procédé Do';
3) Si d(t-1)=1 remplacer Q par Q+P en utilisant le procédé Ad;
4) Pour i allant de t-2 à 0 exécuter :
4a) Remplacer Q par 2Q;
4b) Si d(i)=1 remplacer Q par Q+P;
5) Retourner Q.

Plus généralement, le procédé de la première variante décrit précédemment s'applique à l'opération de multiplication scalaire quelque soit le procédé (noté par la suite A) utilisé pour réaliser le calcul de la multiplication scalaire. Le procédé A fait appel aux opérations Do et Ad définies précédemment.

La première variante de la contre mesure consiste à remplacer la première opération Do par Do' définie précédemment.

La première variante permet donc d'assurer que les variables intermédiaires manipulées lors de l'opération de multiplication scalaire sont aléatoires. Cela rend l'attaque DPA précédemment décrite inapplicable.

Dans ce paragraphe on décrit la deuxième variante de modification de l'opération de multiplication scalaire.

La deuxième variante consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul et à la fin du procédé de calcul. Dans le cas de l'utilisation de l'algorithme " double and add ", le procédé modifié de multiplication scalaire est le suivant en 7 étapes. Le procédé prend en entrée un point P et un entier d L'entier d est noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme retourne en sortie le point Q=d.P.

Cette seconde variante s'exécute en sept étapes:

1) Initialiser le point Q avec la valeur P;

2) Remplacer Q par 2.Q en utilisant le procédé Do';

3) Si d(t-1)=1 remplacer Q par Q+P en utilisant le procédé Ad;

4) Pour i allant de t-2 à 1 exécuter :
   4a) Remplacer Q par 2Q;
   4b) Si d(i)=1 remplacer Q par Q+P;
5) Remplacer Q par 2.Q en utilisant le procédé Do';
6) Si d(0)=1 remplacer Q par Q+P en utilisant le procédé Ad;
7) Retourner Q.

Plus généralement, le procédé de la deuxième variante décrit précédemment s'applique à l'opération de multiplication scalaire quelque soit le procédé (noté par la suite A) utilisé pour réaliser le calcul de la multiplication scalaire. Le procédé A fait appel aux opérations Do et Ad définies précédemment. La deuxième variante de la contre mesure consiste à remplacer la première opération Do par Do' définie précédemment et la dernière opération Do par Do'.

La deuxième variante permet donc d'assurer que les variables intermédiaires manipulées lors de l'opération de multiplication scalaire sont aléatoires. L'avantage de la deuxième variante est une sécurité accrue contre des attaques DPA en fin d'algorithme de multiplication scalaire. En particulier, la deuxième variante rend l'attaque DPA précédemment décrite inapplicable.

Dans ce paragraphe, on décrit la troisième variante de modification de l'opération de multiplication scalaire.

La troisième variante consiste à rendre aléatoire la représentation de chacun des points manipulés au cours du procédé de multiplication scalaire. Dans le cas de l'utilisation de l'algorithme " double and add ", le procédé modifié de multiplication scalaire est le suivant en 4 étapes. Le procédé prend en entrée un point P et un entier d. L'entier d est noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme retourne en sortie le point Q=d.P.

Cette troisième variante s'exécute en trois étapes:

1) Initialiser le point Q avec le point P;
2) Pour i allant de t-2 à 0 exécuter :
2a) Remplacer Q par 2Q en utilisant le procédé Do';
2b) Si d(i)=1 remplacer Q par Q+P en utilisant le procédé Ad';
3) Retourner Q.

Plus généralement, le procédé de la troisième variante décrit précédemment s'applique à l'opération de multiplication scalaire quelque soit le procédé (noté par la suite A) utilisé pour réaliser le calcul de la multiplication scalaire. Le procédé A fait appel aux opérations Do et Ad définies précédemment.

La troisième variante de la contre mesure consiste à remplacer toutes les opérations Do par Do' et Ad par Ad'.

La troisième variante permet donc d'assurer que les variables intermédiaires manipulées lors de l'opération de multiplication scalaire sont aléatoires. L'avantage de la troisième variante par rapport à la deuxième variante est une sécurité accrue contre les attaques DPA sur les opérations intermédiaires du procédé de multiplication scalaire. En particulier, la troisième variante rend l'attaque DPA précédemment décrite inapplicable.

Dans ce paragraphe on décrit la quatrième variante de modification de l'opération de multiplication scalaire. La quatrième variante consiste à rendre aléatoire la représentation de chacun des points manipulés au cours du procédé de multiplication scalaire. La quatrième variante est une modification de la troisième variante par l'utilisation d'un compteur, ledit compteur permettant de déterminer les étapes de l'algorithme de multiplication scalaire pour lesquelles la représentation d'un point est rendue aléatoire. On définit pour cela un paramètre de sécurité T. Dans la pratique on peut prendre T=5. Dans le cas de l'utilisation de l'algorithme " double and add ", le procédé modifié de multiplication scalaire est le suivant en 4 étapes. Le procédé prend en entrée un point P et un entier d.

L'entier d est noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme retourne en sortie le point Q=d.P.

La quatrième variante s'exécute en trois étapes:

1) Initialiser le point Q avec le point P
2) Initialiser le compteur co à la valeur T.
3) Pour i allant de t-1 à 0 exécuter :
3a) Remplacer Q par 2Q en utilisant le procédé Do si co est différent de 0, sinon utiliser le procédé Do'.
3b) Si d(i)=1 remplacer Q par Q+P en utilisant le procédé Ad.
3c) Si co=0 alors réinitialiser le compteur co à la valeur T.
3d) Décrémenter le compteur co.
3) Retourner Q.

Plus généralement, le procédé de la troisième variante décrit précédemment s'applique à l'opération de multiplication scalaire quelque soit le procédé (noté par la suite A) utilisé pour réaliser le calcul de la multiplication scalaire. Le procédé A fait appel aux opérations Do et Ad définies précédemment.
La variante de la troisième contre mesure consiste à initialiser un compteur co à la valeur T. L'opération Do est remplacée par l'opération Do' si la valeur du compteur est égale à 0.

Après chaque exécution des opérations Do ou Do', le compteur est réinitialisé à la valeur T s'il a atteint la valeur 0 ; il est ensuite décrémenté.

La quatrième variante permet donc d'assurer que les variables intermédiaires manipulées lors de l'opération de multiplication scalaire sont aléatoires. L'avantage de la quatrième variante par rapport à la troisième variante est une plus grande rapidité d'exécution. La quatrième variante rend l'attaque DPA précédemment décrite inapplicable.

L'application de l'une des 4 variantes précédemment décrite permet donc de protéger tout algorithme cryptographique basé sur les courbes elliptiques contre l'attaque de type DPA précédemment décrite.

REVENDICATIONS

1- Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique de type courbe élliptique en utilisant la représentation des points de ladite courbe elliptique en coordonnées projectives consistant à représenter un point P de la courbe elliptique par les coordonnées (X, Y, Z) telles que x=X/Z et y=Y/Z^3, x et y étant les coordonnées du point de la courbe elliptique en coordonnées affines, ladite courbe comprenant n éléments et étant définie sur un corps fini GF(p), p étant un nombre premier, ladite courbe ayant pour équation y^2=x^3+a*x+b, ou définie sur un corps fini GF(2^n), ladite courbe ayant pour équation y^2+x*y=x^3+a*x^2+b, où a et b sont des paramètres entiers fixés au départ,
ledit procédé étant caractérisé en ce qu'il choisit un représentant aléatoire parmi n éléments possibles en coordonnées projectives de la courbe élliptique et consiste en une modification des opérations d'addition de points et le doublement desdits points et une modification de l'opération de multiplication scalaire.

2- Procédé de contre-mesure selon la revendication 1caractérisé en ce que le procédé de la contre mesure s'applique quelque soit le procédé ou algorithme, noté par la suite A, utilisé pour réaliser l'opération de doublement de point, le procédé A étant remplacé par le procédé A' en 3 étapes, en utilisant une entrée définie par un point P=(X1,Y1,Z1) représenté en coordonnées projectives et une sortie définie par un point Q=(X2,Y2,Z2) représenté en coordonnés projectives tel que Q=2.P, de la courbe elliptique, lesdites étapes étant:

1) Tirer au hasard un entier λ tel que 0<λ<p;
2) Calculer X'1=λ^2*X1, Y'1=λ^3*Y1 et Z'1=λ*Z1, X'1, Y'1 et Z'1 définissant les coordonnées du point P'=(X'1,Y'1,Z'1);
3) Calculer Q=2*P' à l'aide de l'algorithme A.

3- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que l'algorithme de doublement de points, ou opérations de doublement de points d'une courbe elliptique défini sur ledit corps fini GF(p) s'effectue en huit étapes:

1) Tirer au hasard un entier λ tel que 0<λ<p;
2) Calculer X'1=λ^2*X1, Y'1=λ^3*Y1 et Z'1=λ*Z1;
3) Calculer M=3*X'1^2+a*Z'1^4;
4) Calculer Z2=2*Y'1*Z'1;
5) Calculer S=4*X'1*Y'1^2;
6) Calculer X2=M^2-2*S;
7) Calculer T=8*Y'1^4;
8) Calculer Y2=M*(S-X2)-T.

4- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que plus généralement le procédé dela contre-mesure s'applique quelque soit le procédé noté par la suite A utilisé pour réaliser l'opération d'addition de points sur une courbe elliptique défini sur ledit corps fini GF(p) s'effectue en cinq étapes :

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par λ*Z0;

3) Tirer au hasard un élément μ non nul de GF(2^n);

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par μ*Z1;

5) Calcul de R=P+Q à l'aide de l'algorithme A.

5- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini GF(p), où p est un nombre premier, est la suivante: les coordonnées projectives du point R=(X2,Y2,Z2) tel que R=P+Q avec P=(X0,Y0,Z0) et Q=(X1,Y1,Z1) sont calculées par le procédé suivant en 16 étapes, dans chacune des étapes, les calculs étant effectués modulo p:

1) Tirer au hasard un entier λ appartenant audit corp fini GF(p) tel que 0<λ<p;

2) Remplacer X0 par λ^2*X0,Y0 par λ^3*Y0 et Z0 par λ Z0;

3) Tirer au hasard un entier μ apppartenant à tel que $0<\mu<p$;

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par $\mu*Z1$;

5) Calculer $U0=X0*Z1^2$;

6) Calculer $S0=Y0*Z1^3$;

7) Calculer $U1=X1*Z0^2$;

8) Calculer $S1=Y1*Z0^3$;

9) Calculer $W=U0-U1$;

10) Calculer $R=S0-S1$;

11) Calculer $T=U0+U1$;

12) Calculer $M=S0+S1$;

13) Calculer $Z2=Z0*Z1*W$;

14) Calculer $X2=R^2-T*W^2$;

15) Calculer $V=T*W^2-2*X2$;

16) Calculer $2*Y2=V*R-M*W^3$.

6- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que plus généralement, la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini $GF(2^n)$, où n est un nombre premier, est la suivante: les coordonnées projectives du point $P=(X1,Y1,Z1)$ tel que $R=P+Q$ et $Q=(X2,Y2,Z2)$ sont calculées par le procédé suivant en 3 étapes, dans chacune des étapes, les calculs étant effectués modulo p:

1) Tirer au hasard un élément λ non nul de $GF(2^n)$;

2) Calculer $X'1=\lambda^2*X1$, $Y'1=\lambda^3*Y1$, $Z'1=\lambda*Z1$, $X'1$, $Y'1$ et $Z'1$ définissent les coordonnées du point $P'=(X'1,Y'1,Z'1)$;

3) Calcul de $Q=2.P'$ à l'aide de l'algorithme A.

7- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que le procédé de la contre mesure consiste en une modification du procédé précédent, le nouveau procédé de doublement de point d'une courbe elliptique étant définie sur le corps fini GF(2^n), et consiste en les 6 étapes suivantes :

1) Tirer au hasard un élément non nul λ de GF(2^n);

2) Calculer $X'1=\lambda^2*X1$, $Y'1=\lambda^3*Y1$, $Z'1=\lambda*Z1$;

3) Calculer $Z2=X'1*Z'1^2$;

4) Calculer $X2=(X'1+c*Z'1^2)^4$;

5) Calculer $U=Z2+X'1^2+Y'1*Z'1$;

6) Calculer $Y2=X'1^4*Z2+U*X2$.

8 - Procédé de contre-mesure selon la revendication 1 caractérisé en ce que
Plus généralement, la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini GF(2^n), où n est un nombre premier, est la suivante: les coordonnées projectives du point P=(X0,Y0,Z0) et Q=(X1,Y1,Z2) en entrée et R=(X2,Y2,Z2) sont calculées par le procédé suivant en 5 étapes, dans chacune des étapes, les calculs étant effectués modulo:

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par $\lambda*Z0$;

3) Tirer au hasard un élément μ non nul de GF(2^n);

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par $\mu*Z1$;

5) Calcul de R=P+Q à l'aide de l'algorithme A.

9- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que le procédé de la contre mesure consiste en une modification du procédé d'addition de points d'une courbe elliptique définie sur le corps fini GF(2^n)et consiste en les 16 étapes suivantes :

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par $\lambda*Z0$;

3) Tirer au hasard un élément μ non nul de GF(2^n);

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par $\mu*Z1$;

5) Calculer U0=X0*Z1^2;

6) Calculer S0=Y0*Z1^3;

7) Calculer U1=X1*Z0^2;

8) Calculer S1=Y1*Z0^3;

9) Calculer W=U0+U1;

10) Calculer R=S0+S1;

11) Calculer L=Z0*W;

12) Calculer V=R*X1+L*Y1;

13) Calculer Z2=L*Z1;

14) Calculer T=R+Z2;

15) Calculer X2=a*Z2^2+T*R+W^3;

16) Calculer Y2=T*X2+V*L^2;

10 - Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la première variante de modification de l'opération de multiplication scalaire consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul par l'utilisation de l'algorithme " double and add ", le procédé modifié , de multiplication scalaire est le suivant en 5 étapes, en prenant en entrée un point P et un entier d,l'entier d étant noté d=(d(t),d(t-1),..., d(0)), où (d(t),d(t-1),...,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible, l'algorithme retournant en sortie le point Q=d.P, le procédé Do étant le procédé de doublement de points, le procédé Do' étant le procédé de doublement des points modifiés suivant l'une quelconque des revendications précédentes, cette première variante s'exécutant en cinq étapes:

1) Initialiser le point Q avec la valeur P;

2) Remplacer Q par 2.Q en utilisant le procédé Do';

3) Si d(t-1)=1 remplacer Q par Q+P en utilisant le procédé Ad, le procédé Ad étant le procédé d'addition de points;

4) Pour i allant de t-2 à 0 exécuter :

4a) Remplacer Q par 2Q;

4b) Si d(i)=1 remplacer Q par Q+P;

5) Retourner Q.

11- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la deuxième variante de l'opération de multiplication scalaire consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul et à la fin du procédé de calcul, ceci dans le cas de l'utilisation de l'algorithme " double and add ",
le procédé modifié de multiplication scalaire étant le suivant en 7 étapes, prenant en entrée un point P et un entier d, l'entier d étant noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible, l'algorithme retournant en sortie le point Q=d.P, ladite seconde variante s'exécutant en sept étapes:

1) Initialiser le point Q avec la valeur P;
2) Remplacer Q par 2.Q en utilisant le procédé Do';
3) Si d(t-1)=1 remplacer Q par Q+P en utilisant le procédé Ad;
4) Pour i allant de t-2 à 1 exécuter :
   4a) Remplacer Q par 2Q;
   4b) Si d(i)=1 remplacer Q par Q+P;
5) Remplacer Q par 2.Q en utilisant le procédé Do';
6) Si d(0)=1 remplacer Q par Q+P en utilisant le procédé Ad;
7) Retourner Q.

12- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la troisième variante de l'opération de multiplication scalaire s'exécute en trois étapes:

1) Initialiser le point Q avec le point P;
2) Pour i allant de t-2 à 0 exécuter :
2a) Remplacer Q par 2Q en utilisant le procédé Do';
2b) Si d(i)=1 remplacer Q par Q+P en utilisant le procédé Ad', Ad' étant le procédé d'addition des points modifiés suivant les revendications précédentes;
3) Retourner Q.

13- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la quatrième variante de l'opération de multiplication scalaire s'exécute en trois étapes:
1) Initialiser le point Q avec le point P
2) Initialiser le compteur co à la valeur T.
3) Pour i allant de t-1 à 0 exécuter :
3a) Remplacer Q par 2Q en utilisant le procédé Do si co est différent de 0, sinon utiliser le procédé Do'.
3b) Si d(i)=1 remplacer Q par Q+P en utilisant le procédé Ad.
3c) Si co=0 alors réinitialiser le compteur co à la valeur T.
3d) Décrémenter le compteur co.
3) Retourner Q.

14- Composant électronique utilisant le procédé selon l'une quelconque des revedications précédentes caractérisé en ce qu'il peut être une carte à puce.

INTERNATIONAL SEARCH REPORT

[redacted]

Int[redacted] Application No
PCT/FR 00/00603

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MENEZES A J ET AL: "ELLIPTIC CURVE CRYPTOSYSTEMS AND THEIR IMPLEMENTATION" JOURNAL OF CRYPTOLOGY,US,NEW YORK, NY, vol. 6, no. 4, September 1993 (1993-09), pages 209-224, XP002069135 abstract page 209, last paragraph -page 210, paragraph 1 page 216, line 17 -page 217, line 15	1

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2000	09/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

[redacted]

De[redacted]rnationale No
PCT/FR 00/00603

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/30 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MENEZES A J ET AL: "ELLIPTIC CURVE CRYPTOSYSTEMS AND THEIR IMPLEMENTATION" JOURNAL OF CRYPTOLOGY,US,NEW YORK, NY, vol. 6, no. 4, septembre 1993 (1993-09), pages 209-224, XP002069135 abrégé page 209, dernier alinéa -page 210, alinéa 1 page 216, ligne 17 -page 217, ligne 15	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
31 mai 2000	09/06/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

Translation

09/937390

RECEIVED

FEB 0 4 2002

Technology Center 2100

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM0655	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00603	International filing date (*day/month/year*) 13 March 2000 (13.03.00)	Priority date (*day/month/year*) 26 March 1999 (26.03.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/30, G06F 7/72		
Applicant GEMPLUS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 9 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
23 September 2000 (23.09.00)	06 June 2001 (06.06.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

International application No.
PCT/FR00/00603

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-29, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-13, filed with the letter of 02 May 2001 (02.05.2001),
Nos. _____, filed with the letter of _____.

☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☒ the claims, Nos. 14
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 00/00603

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-13	YES
	Claims		NO
Inventive step (IS)	Claims	1-13	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-13	YES
	Claims		NO

2. Citations and explanations

The invention concerns a countermeasure process (Claim 1) for electronic components (e.g. chip card) implementing an encryption algorithm with a public key of the elliptical curve type, as well as an electronic component using this process (use Claim 13).

Prior art:

The article by MENEZES (D1) describes an encryption algorithm with a public key of the elliptical curve type using the representation of the points of said elliptical curve in a system of projection co-ordinates and performing operations of point duplication, point addition and scalar multiplication of the points on the elliptical curve.

Problem:

The implementation on a chip card of such an algorithm is open to so-called DPA attacks, which consist in a differential analysis of the power consumption of the data processing microprocessor and enable the private encryption key to be found.

This Page Blank (uspto)

Invention:

Claim 1 defines a countermeasure process to ward off such attacks. This process is based on the choice of a random representative of a point on the elliptical curve on which calculation is performed and comprises a modified point duplication operation as defined in the characterising portion of the claim.

Thus, the choice of a random representative of a point on which calculation is performed makes the intermediate calculated values random as well and hence invulnerable to DPA attacks.

This approach is not known and cannot be derived from the single search report citation, document D1.

Claims 2 to 12 are dependent on Claim 1 and therefore also meet the PCT requirements for novelty and inventive step, as well as use Claim 13.

VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claim 1 does not entirely meet the requirements of PCT Article 6 for clarity because the modifications to the point addition and scalar multiplication operations are not defined in Claim 1 but rather in the dependent claims. As a result, the restrictions intended by these features are not clear from this claim, which therefore contravenes PCT Article 6.

TRANSLATION OF ANNEX TO

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

CLAIMS

1. A countermeasure method in an electronic component implementing an elliptical curve type public key encryption algorithm using the representation of the points of the said elliptical curve in projective coordinates, consisting in representing a point P on the elliptical curve by the coordinates (X, Y, Z) such that x=X/Z and y=Y/Z^3, x and y being the coordinates of the point on the elliptical curve in terms of affine coordinates, the said curve comprising n elements and being defined on a finite field GF(p), p being a prime number, the said curve having the equation y^2=x^3+a*x+b, or defined on a finite field GF(2^n), the said curve having the equation y^2+x*y=x^3+a*x^2+b, where a and b are integer parameters fixed at the start,

the said method being characterised in that it chooses a random representative from amongst n possible elements in terms of projective coordinates of the elliptical curve and consists of a modification of the operations of addition of points and doubling of the said points and a modification of the scalar multiplication operation.

2. A countermeasure method according to Claim 1, characterised in that the countermeasure applies whatever the method or algorithm, hereinafter denoted A, used for performing the point doubling operation, the method A being replaced by the method A' in three steps, using an input defined by a point P=(X1,Y1,Z1)

This Page Blank (uspto)

represented in terms of projective coordinates and an output defined by a point Q=(X2,Y2,Z2) represented in terms of projective coordinates, such that Q=2.P, of the elliptical curve, the said steps being:

1) Drawing at random an integer λ such that 0<λ<p;

2) Calculating X'1=λ^2*X1, Y'1=λ^3*Y1 and Z'1=λ*Z1, X'1, Y'1 and Z'1 defining the coordinates of the point P'=(X'1,Y'1,Z'1);

3) Calculating Q=2*P' by means of the algorithm A.

3. A countermeasure method according to Claim 1, characterised in that the point doubling algorithm, or operations of doubling points on an elliptical curve defined on the said finite field GF(p), is effected in eight steps:

1) Drawing at random an integer λ such that 0<λ<p;

2) Calculate X'1=λ^2*X1, Y'1=λ^3*Y1 and Z'1=λ*Z1;

3) Calculate M=3*X'1^2+a*Z'1^4;

4) Calculate Z2=2*Y'1*Z'1;

5) Calculate S=4*X'1*Y'1^2;

6) Calculate X2=M^2-2*S;

7) Calculate T=8*Y'1^4;

8) Calculate Y2=M*(S-X2)-T.

4. A countermeasure method according to Claim 1, characterised in that more generally the countermeasure method applies whatever the method denoted hereinafter A used for performing the points addition operation on

an elliptical curve defined on the said finite field GF(p) is effected in five steps:

1) Drawing at random a non-zero integer λ of GF(2^n);

2) Replacing X0 with λ^2*X0, Y0 with λ^3*Y0 and Z0 with λ*Z0;

3) Drawing at random a non-zero integer μ of GF(2^n);

4) Replacing X1 with μ^2*X1, Y1 with μ^3*Y1 and Z1 with μ*Z1;

5) Calculating R=P+Q by means of algorithm A.

5. A countermeasure method according to Claim 1, characterised in that the modification of the point addition algorithm for an elliptical curve defined on the finite field GF(p), where p is a prime number, is as follows: the projective coordinates of the point R=(X2,Y2,Z2) such that R=P+Q with P=(X0,Y0,Z0) and Q=(X1,Y1,Z1) are calculated by the following method in 16 steps, in each of the steps the calculations being effected modulo p:

1) Drawing at random an integer λ belonging to the finite field GF(p) such that 0<λ<p;

2) Replacing X0 with λ^2*X0, Y0 with λ^3*Y0 and Z0 with λ*Z0;

3) Drawing at random an integer μ such that 0<μ<p;

4) Replacing X1 with μ^2*X1, Y1 with μ^3*Y1 and Z1 with μ*Z1;

5) Calculate U0=X0*Z1^2;

6) Calculate S0=Y0*Z1^3;

7) Calculate U1=X1*Z0^2;

8) Calculate S1=Y1*Z0^3;

9) Calculate W=U0-U1;

10) Calculate R=S0-S1;

11) Calculate T=U0+U1;

12) Calculate M=S0+S1;

13) Calculate Z2=ZO*Z1*W;

14) Calculate X2=R^2-T*W^2;

15) Calculate V=T*W^2-2*X2;

16) Calculate 2*Y2=V*R-M*W^3.

6. A countermeasure method according to Claim 1, characterised in that, more generally, the modification of the point addition algorithm for an elliptical curve defined on the finite field GF(2^n), where n is a prime number, is as follows: the projective coordinates of the point P=(X1,Y1,Z1) such that R=P+Q and Q=(X2,Y2,Z2) are calculated by the following method in 3 steps, in each of the steps the calculations being carried out modulo p:

1) Drawing at random a non-zero element λ of GF(2^n);

2) Calculating $X'1=\lambda^2*X1$, $Y'1=\lambda^3*Y1$ and $Z'1=\lambda*Z1$, X'1, Y'1 and Z'1 defining the coordinates of the point P'=(X'1,Y'1,Z'1);

3) Calculating Q=2.P' by means of the algorithm A.

7. A countermeasure method according to Claim 1, characterised in that the countermeasure method

consists of a modification of the previous method, the new point doubling method for an elliptical curve being defined on the finite field GF(2^n), and consists of the following 6 steps:

1) Drawing at random a non-zero element λ of GF(2^n);

2) Calculate X'1=λ^2*X1, Y'1=λ^3*Y1, Z'1=λ*Z1;

3) Calculate Z2=X'1*Z'1^2;

4) Calculate X2=(X'1+c*Z'1^2)^4;

5) Calculate U=Z2+X'1^2+Y'1*Z'1;

6) Calculate Y2=X'1^4*Z2+U*X2.

8. A countermeasure method according to Claim 1, characterised in that, more generally, the modification of the point addition algorithm for an elliptical curve defined on the finite field GF(2^n), where n is a prime number, is as follows: the projective coordinates of the point P=(X0,Y0,Z0) and Q=(X1,Y1,Z2) at the input and R=(X2,Y2,Z2) are calculated by the following method in 5 steps, in each of the steps the calculations being carried out modulo:

1) Drawing at random a non-zero element λ of GF(2^n);

2) Replacing X0 with λ^2*X0, Y0 with λ^3*Y0 and Z0 with λ*Z0;

3) Drawing at random a non-zero element μ of GF(2^n);

4) Replacing X1 with μ^2*X1, Y1 with μ^3*Y1 and Z1 with μ*Z1;

5) Calculating R=P+Q using the algorithm A.

9. A countermeasure method according to Claim 1, characterised in that the countermeasure method consists of a modification of the point addition method for an elliptical curve defined on the finite field GF(2^n) and consists of the following 16 steps:

1) Drawing at random a non-zero element λ of GF(2^n);

2) Replacing X0 with λ^2*X0, Y0 with λ^3*Y0 and Z0 with λ*Z0;

3) Drawing at random a non-zero element μ of GF(2^n);

4) Replacing X1 with μ^2*X1, Y1 with μ^3*Y1 and Z1 with μ*Z1;

5) Calculate U0=X0*Z1^2;

6) Calculate S0=Y0*Z1^3;

7) Calculate U1=X1*Z0^2;

8) Calculate S1=Y1*Z0^3;

9) Calculate W=U0+U1;

10) Calculate R=S0+S1;

11) Calculate L=Z0*W;

12) Calculate V=R*X1+L*Y1;

13) Calculate Z2=L*Z1;

14) Calculate T=R+Z2;

15) Calculate X2=a*Z2^2+T*R+W^3;

16) Calculate Y2=T*X2+V*L^2.

10. A countermeasure method according to Claim 1, characterised in that the first variant of a modification of the scalar multiplication operation consists in making random the representation of a point

at the start of the calculation method by the use of the "double and add" algorithm, the modified method of scalar multiplication is as follows in 5 steps, taking as an input a point P and an integer d, the integer d being denoted d=(d(t),d(t-1),…,d(0)), where (d(t),d(t-1),…,d(0)) is the binary representation of d, with d(t) the most significant bit and d(0) the least significant bit, the algorithm returning as an output the point Q=d.P, the method Do being the points doubling method, the method Do' being the modified points doubling method according to any one of the preceding claims, this first variant being executed in five steps:

1) Initialising the point Q with the value P;

2) Replacing Q with 2.Q using the method Do';

3) If d(t-1)=1 replacing Q with Q+P using the method Ad;

4) For i ranging from t-2 to 0 executing:

4a) Replacing Q with 2Q;

4b) If d(i)=1, replacing Q with Q+P;

5) Returning Q.

11. A countermeasure method according to Claim 1, characterised in that the second variant of the scalar multiplication operation consists in making random the representation of a point at the start of the calculation method and at the end of the calculation method, this in the case of the use of the "double and add" algorithm,

the modified scalar multiplication method being the following one in 7 steps, taking as an input a point P and an integer d, the integer d being denoted

d=(d(t),d(t-1),…,d(0)), where (d(t),d(t-1),…,d(0)) is the binary representation of d, with d(t) the most significant bit and d(0) the least significant bit, the algorithm returning as an output the point Q=d.P, the said second variant being executed in seven steps:

1) Initialising the point Q with the value P;

2) Replacing Q with 2.Q using the method Do';

3) If d(t-1)=1, replacing Q with Q+P using the method Ad;

4) For i ranging from t-2 to 1, executing:

4a) Replacing Q with 2Q;

4b) If d(i)=1, replacing Q with Q+P;

5) Replacing Q with 2.Q using the method Do';

6) If d(0)=1, replacing Q with Q+P using the method Ad;

7) Returning Q.

12. A countermeasure method according to Claim 1, characterised in that the third variant of the scalar multiplication operation is executed in three steps:

1) Initialising the point Q with the point P;

2) For i ranging from t-2 to 0, executing:

2a) Replacing Q with 2Q using the method Do';

2b) If d(i)=1, replacing Q with Q+P using the method Ad', Ad' being the method of addition of the modified points according to the preceding claims;

3) Returning Q.

13. A countermeasure method according to Claim 1, characterised in that the fourth variant of the

scalar multiplication operation is executed in three steps:

1) Initialising the point Q with the point P.

2) Initialising the counter co to the value T.

3) For i ranging from t-1 to 0, executing:

3a) Replacing Q with 2Q using the method Do if co is different from 0, otherwise using the method Do'.

3b) If d(i)=1, replacing Q with Q+P using the method Ad.

3c) If co=0 then reinitialising the counter co to the value T.

3d) Decrementing the counter co.

3) Returning Q.

14. An electronic component using the method according to any one of the preceding claims, characterised in that it can be a smart card.

15 T

rem

TRAITE [redacted] OPERATION EN MATIE[redacted]E BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 655	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00603	Date du dépot international *(jour/mois/année)* 13/03/2000	Date de priorité *(jour/mois/année)* 26/03/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/30		
Déposant GEMPLUS et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 9 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
23/09/2000	06.06.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00603

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-29 version initiale

Revendications, N°:

1-13 reçue(s) le 02/05/2001 avec la lettre du 02/05/2001

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :
   ☒ des revendications, n^{os} : 14
   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-13
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-13
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-13
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) de contre-mesure pour composant électronique (par ex. carte à puce) mettant en oeuvre un algorithme de chiffrement à clé publique de type courbe elliptique, ainsi qu'un composant électronique utilisant ce procédé (revendication d'utilisation 13).

Etat de la technique:

L'article de MENEZES (= D1) décrit un algorithme de cryptographie à clé publique de type courbe elliptique en utilisant la représentation des points de ladite courbe elliptique en coordonnées projectives et utilisant des opérations de doublement de points, d'addition de points et de multiplication scalaire de points de la courbe elliptique.

Problème:

L'implémentation sur carte à puce d'un tel algorithme est vulnérable à des attaques dites DPA consistant en une analyse différentielle de consommation de courant du microprocesseur manipulant les données et permettant de retrouver la clé privée de chiffrement.

Invention:

La revendication 1 définit un procédé de contre-mesure pour parer à ces attaques, basé sur le choix d'un représentant aléatoire d'un point de la courbe elliptique sur lequel on effectue un calcul et comportant une opération de doublement de points modifiée telle que définie dans la partie caractérisante de la revendication.
Ainsi, en choisissant un représentant aléatoire d'un point sur lequel on effectue un calcul, les valeurs intermédiaires du calcul deviennent elles-mêmes aléatoires et donc insensibles aux attaques DPA.
Une telle démarche n'est pas connue ni dérivable de l'unique document D1 cité dans le rapport de recherche.

This Page Blank (usp[illegible]

Les revendications 2 à 12 sont respectivement dépendantes de la revendication 1 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive, ainsi que la revendication d'utilisation 13.

Concernant le point VIII
Observations relatives à la demande internationale

La revendication 1 ne remplit pas entièrement les conditions de l'article 6 PCT relative à la clarté. En effet, les modifications des opérations d'addition de points et de multiplication scalaire ne sont pas définies dans la revendication 1 mais dans des revendications dépendantes. De ce fait les limitations que l'on entend définir par ces caractéristiques ne ressortent pas clairement de cette revendication, contrairement à ce qui est exigé à l'article 6 PCT.

REVENDICATIONS

1- Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique de type courbe élliptique en utilisant la représentation des points de ladite courbe elliptique en coordonnées projectives consistant à représenter un point P de la courbe elliptique par les coordonnées (X, Y, Z) telles que x=X/Z et y=Y/Z^3, x et y étant les coordonnées du point de la courbe elliptique en coordonnées affines, ladite courbe comprenant n éléments et étant définie sur un corps fini GF(p), p étant un nombre premier, ladite courbe ayant pour équation y^2=x^3+a*x+b, ou définie sur un corps fini GF(2^n), ladite courbe ayant pour équation y^2+x*y=x^3+a*x^2+b, où a et b sont des paramètres entiers fixés au départ, ledit procédé choisissant un représentant entier aléatoire parmi n éléments possibles en coordonnées projectives de la courbe elliptique et consistant en une modification des opérations d'addition de points, de doublement desdits points et/ou une modification de l'opération de multiplication scalaire, caractérisé en ce que le procédé de la contre mesure s'applique quelque soit le procédé ou l'algorithme, noté par la suite A, utilisé pour réaliser l'opération de doublement de point, le procédé A étant remplacé par le procédé A' en 3 étapes, en utilisant une entrée définie par un point P=(X1,Y1,Z1) représenté en coordonnées projectives et une sortie définie par un point

Q=(X2,Y2,Z2) représenté en coordonnés projectives tel que Q=2.P, de la courbe elliptique, lesdites étapes étant:

1) Tirer au hasard un entier λ tel que 0<λ<p;
2) Calculer X'1=λ^2*X1, Y'1=λ^3*Y1 et Z'1=λ*Z1, X'1, Y'1 et Z'1 définissant les coordonnées du point P'=(X'1,Y'1,Z'1);
3) Calculer Q=2*P' à l'aide de l'algorithme A.

2- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que l'algorithme de doublement de points, ou opérations de doublement de points d'une courbe elliptique défini sur ledit corps fini GF(p) s'effectue en huit étapes:

1) Tirer au hasard un entier λ tel que 0<λ<p;
2) Calculer X'1=λ^2*X1, Y'1=λ^3*Y1 et Z'1=λ*Z1;
3) Calculer M=3*X'1^2+a*Z'1^4;
4) Calculer Z2=2*Y'1*Z'1;
5) Calculer S=4*X'1*Y'1^2;
6) Calculer X2=M^2-2*S;
7) Calculer T=8*Y'1^4;
8) Calculer Y2=M*(S-X2)-T.

3- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que plus généralement le procédé de la contre-mesure s'applique quelque soit le procédé noté par la suite A utilisé pour réaliser l'opération d'addition de points sur une courbe elliptique défini sur ledit corps fini GF(p) s'effectue en cinq étapes :

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par λ*Z0;

3) Tirer au hasard un élément μ non nul de GF(2^n);

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par μ*Z1;

5) Calcul de R=P+Q à l'aide de l'algorithme A.

4- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini GF(p), où p est un nombre premier, est la suivante: les coordonnées projectives du point R=(X2,Y2,Z2) tel que R=P+Q avec P=(X0,Y0,Z0) et Q=(X1,Y1,Z1) sont calculées par le procédé suivant en 16 étapes, dans chacune des étapes, les calculs étant effectués modulo p:

1) Tirer au hasard un entier λ appartenant audit corps fini GF(p) tel que 0<λ<p;

2) Remplacer X0 par λ^2*X0,Y0 par λ^3*Y0 et Z0 par λ Z0;

3) Tirer au hasard un entier μ appartenant à tel que 0<μ<p;

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par μ*Z1;

5) Calculer U0=X0*Z1^2;

6) Calculer S0=Y0*Z1^3;

7) Calculer U1=X1*Z0^2;

8) Calculer S1=Y1*Z0^3;

This Page Blank (uspto)

9) Calculer W=U0-U1;

10) Calculer R=S0-S1;

11) Calculer T=U0+U1;

12) Calculer M=S0+S1;

13) Calculer Z2=Z0*Z1*W;

14) Calculer X2=R^2-T*W^2;

15) Calculer V=T*W^2-2*X2;

16) Calculer 2*Y2=V*R-M*W^3.

5- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que plus généralement, la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini GF(2^n), où n est un nombre premier, est la suivante: les coordonnées projectives du point P=(X1,Y1,Z1) tel que R=P+Q et Q=(X2,Y2,Z2) sont calculées par le procédé suivant en 3 étapes, dans chacune des étapes, les calculs étant effectués modulo p:

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Calculer X'1=λ^2*X1, Y'1=λ^3*Y1, Z'1=λ*Z1, X'1, Y'1 et Z'1 définissent les coordonnées du point P'=(X'1,Y'1,Z'1);

3) Calcul de Q=2.P' à l'aide de l'algorithme A.

6- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que le procédé de la contre mesure consiste en une modification du procédé précédent, le nouveau procédé de doublement de point d'une courbe elliptique étant définie sur le corps fini GF(2^n), et consiste en les 6 étapes suivantes :

1) Tirer au hasard un élément non nul λ de GF(2^n);

2) Calculer X'1=λ^2*X1, Y'1=λ^3*Y1, Z'1=λ*Z1;

3) Calculer Z2=X'1*Z'1^2;

4) Calculer X2=(X'1+c*Z'1^2)^4;

5) Calculer U=Z2+X'1^2+Y'1*Z'1;

6) Calculer Y2=X'1^4*Z2+U*X2.

7- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que plus généralement, la modification de l'algorithme d'addition de point d'une courbe elliptique définie sur le corps fini GF(2^n), où n est un nombre premier, est la suivante: les coordonnées projectives du point P=(X0,Y0,Z0) et Q=(X1,Y1,Z2) en entrée et R=(X2,Y2,Z2) sont calculées par le procédé suivant en 5 étapes, dans chacune des étapes, les calculs étant effectués modulo:

1) Tirer au hasard un élément λ non nul de GF(2^n);

2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par λ*Z0;

3) Tirer au hasard un élément μ non nul de GF(2^n);

4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par μ*Z1;

5) Calcul de R=P+Q à l'aide de l'algorithme A.

8- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que le procédé de la contre mesure consiste en une modification du procédé d'addition de points d'une courbe

elliptique définie sur le corps fini GF(2^n)et consiste en les 16 étapes suivantes :

1) Tirer au hasard un élément λ non nul de GF(2^n);
2) Remplacer X0 par λ^2*X0, Y0 par λ^3*Y0 et Z0 par λ*Z0;
3) Tirer au hasard un élément μ non nul de GF(2^n);
4) Remplacer X1 par μ^2*X1, Y1 par μ^3*Y1 et Z1 par μ*Z1;
5) Calculer U0=X0*Z1^2;
6) Calculer S0=Y0*Z1^3;
7) Calculer U1=X1*Z0^2;
8) Calculer S1=Y1*Z0^3;
9) Calculer W=U0+U1;
10) Calculer R=S0+S1;
11) Calculer L=Z0*W;
12) Calculer V=R*X1+L*Y1;
13) Calculer Z2=L*Z1;
14) Calculer T=R+Z2;
15) Calculer X2=a*Z2^2+T*R+W^3;
16) Calculer Y2=T*X2+V*L^2;

9- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la première variante de modification de l'opération de multiplication scalaire consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul par l'utilisation de l'algorithme " double and add ", le procédé modifié de multiplication scalaire est le suivant en 5 étapes, en prenant en entrée un point P et un entier d,l'entier d étant noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0))

est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible, l'algorithme retournant en sortie le point Q=d.P, le procédé Do étant le procédé de doublement de points, le procédé Do' étant le procédé de doublement des points modifiés suivant l'une quelconque des revendications précédentes, cette première variante s'exécutant en cinq étapes:

1) Initialiser le point Q avec la valeur P;
2) Remplacer Q par 2.Q en utilisant le procédé Do';
3) Si d(t-1)=1 remplacer Q par Q+P en utilisant le procédé Ad, le procédé Ad étant le procédé d'addition de points;
4) Pour i allant de t-2 à 0 exécuter :
   4a) Remplacer Q par 2Q;
   4b) Si d(i)=1 remplacer Q par Q+P;
5) Retourner Q.

10- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la deuxième variante de l'opération de multiplication scalaire consiste à rendre aléatoire la représentation d'un point au début du procédé de calcul et à la fin du procédé de calcul, ceci dans le cas de l'utilisation de l'algorithme " double and add ",
le procédé modifié de multiplication scalaire étant le suivant en 7 étapes, prenant en entrée un point P et un entier d, l'entier d étant noté d=(d(t),d(t-1),..., d(0)), où (d(t),d(t-1),...,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible, l'algorithme retournant en sortie le

point Q=d.P, ladite seconde variante s'exécutant en sept étapes:

1) Initialiser le point Q avec la valeur P;
2) Remplacer Q par 2.Q en utilisant le procédé Do';
3) Si d(t-1)=1 remplacer Q par Q+P en utilisant le procédé Ad;
4) Pour i allant de t-2 à 1 exécuter :
   4a) Remplacer Q par 2Q;
   4b) Si d(i)=1 remplacer Q par Q+P;
5) Remplacer Q par 2.Q en utilisant le procédé Do';
6) Si d(0)=1 remplacer Q par Q+P en utilisant le procédé Ad;
7) Retourner Q.

11-Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la troisième variante de l'opération de multiplication scalaire s'exécute en trois étapes:

1) Initialiser le point Q avec le point P;
2) Pour i allant de t-2 à 0 exécuter :
   2a) Remplacer Q par 2Q en utilisant le procédé Do';
   2b) Si d(i)=1 remplacer Q par Q+P en utilisant le procédé Ad', Ad' étant le procédé d'addition des points modifiés suivant les revendications précédentes;
3) Retourner Q.

12- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la quatrième variante de l'opération de multiplication scalaire s'exécute en 3 étapes:

1) Initialiser le point Q avec le point P

2) Initialiser le compteur co à la valeur T.

3) Pour i allant de t-1 à 0 exécuter :

3a) Remplacer Q par 2Q en utilisant le procédé Do si co est différent de 0, sinon utiliser le procédé Do'.

3b) Si d(i)=1 remplacer Q par Q+P en utilisant le procédé Ad.

3c) Si co=0 alors réinitialiser le compteur co à la valeur T.

3d) Décrémenter le compteur co.

4) Retourner Q.

13- Composant électronique utilisant le procédé selon l'une quelconque des revendications précédentes caractérisé en ce qu'il peut être une carte à puce.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM0655	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/00603	Date du dépôt international *(jour/mois/année)* 13/03/2000	(Date de priorité (la plus ancienne) *(jour/mois/année)* 26/03/1999
Déposant GEMPLUS SA et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 1 feuilles.

☐ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. ☐ **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

   ☒ le texte est approuvé tel qu'il a été remis par le déposant.

   ☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

   ☒ le texte est approuvé tel qu'il a été remis par le déposant

   ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°

   ☐ suggérée par le déposant.

   ☐ parce que le déposant n'a pas suggéré de figure.

   ☐ parce que cette figure caractérise mieux l'invention.

   ☒ Aucune des figures n'est à publier.

09/937396

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

NONNENMACHER, Bernard
Gemplus
Avenue du Pic de Bertagne
Parc d'activités de Gémenos
F-13881 Gémenos
FRANCE

Date d'expédition (jour/mois/année) 27 septembre 2001 (27.09.01)	
Référence du dossier du déposant ou du mandataire GEM0655	**NOTIFICATION IMPORTANTE**
Demande internationale no PCT/FR00/00603	**Date du dépôt international** (jour/mois/année) 13 mars 2000 (13.03.00)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

[X] le déposant [ ] l'inventeur [ ] le mandataire [ ] le représentant commun

Nom et adresse	Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)
GEMPLUS Nonnenmacher, Bernard Avenue du Pic de Bertagne Parc d'activités de Gémenos F-13881 Gémenos FRANCE	FR	FR
	no de téléphone 04.42.36.63.56	
	no de télécopieur 04.42.36.63.43	
	no de téléimprimeur	

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

[ ] la personne [ ] le nom [X] l'adresse [ ] la nationalité [ ] le domicile

Nom et adresse	Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)
GEMPLUS Avenue du Pic de Bertagne Parc d'activités de Gémenos F-13881 Gémenos FRANCE	FR	FR
	no de téléphone 04.42.36.63.56	
	no de télécopieur 04.42.36.63.43	
	no de téléimprimeur	

3. Observations complémentaires, le cas échéant:

4. Une copie de cette notification a été envoyée:

[X] à l'office récepteur
[ ] à l'administration chargée de la recherche internationale
[ ] à l'administration chargée de l'examen préliminaire international
[ ] aux offices désignés concernés
[X] aux offices élus concernés
[ ] autre destinataire:

Bureau international de l'OMPI **34, chemin des Colombettes** **1211 Genève 20, Suisse**	Fonctionnaire autorisé: Philippe Bécamel
no de télécopieur (41-22) 740.14.35	no de téléphone (41-22) 338.83.38